THE DATA SECURITY BREACH

Protections and Responsibilities Under Georgia's Personal Identity Protection Act

By Amy T. Andrews
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
aandrews@bakerdonelson.com

Several recent and infamous data security breaches may lead Georgia consumers and companies alike to wonder "What if someone's personal information is breached?". The Georgia Personal Identity Protection Act of 2005 (the Act), codified at O.C.G.A. § 10-1-911 and § 10-1-912, answers this question.

The Act requires notice of a data breach be provided to individuals whose unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person. Under the Act, Personal Information refers to an individual's first name, or first initial, and last name *in combination* with one or more of the following: (i) Social Security number; (ii) driver's license number or state identification card number; (iii) account number, credit card number or debit card number, if such number could be used without additional identifying information, access codes or passwords; or (iv) account password, personal identification numbers or other access codes. Even when not combined with an individual's name, each of the above items is considered to be Personal Information if the compromise of such information would be sufficient to perform or attempt to perform identity theft against the individual. However, if the name or any of the foregoing items are encrypted or redacted, or the information includes details that are lawfully available from federal, state or local government records, then the information is not considered Personal Information.

Under the Act, the persons or entities responsible for providing notice of a breach (Covered Entities) include any Information Broker or Data Collector that maintains computerized data that includes Personal Information of individuals and any person or business that maintains such data on behalf of an Information Broker or Data Collector. An Information Broker is any person or entity who, for monetary fees or duties, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing Personal Information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

A Data Collector includes any state or local agency or subdivision thereof, including any department, bureau, authority, public university or college, academy, commission or other government entity, unless such entity's records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

Covered Entities must provide notice of any unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of an individual's Personal Information maintained by such Covered Entity. Such notice must be made in the most expedient time possible and without unreasonable delay. Notice may be written, telephonic or electronic, if the electronic notice satisfies the provisions of 15 U.S.C. Section 7001 regarding electronic records and signatures.

Under certain circumstances, Substitute Notice may be given through email notice, conspicuous posting of the notice on the Covered Entity's website page, or notification by way of major state-wide media. Substitute Notice applies if the Covered Entity demonstrates that the costs of providing notice would exceed $50,000, that the affected class of individuals to be notified exceeds 100,000, or that the Covered Entity does not have sufficient contact information to provide written or electronic notice to such individuals.

Any Covered Entity that maintains its own notification procedures as part of an information security policy and is otherwise consistent with the timing requirements of the Act will be deemed in compliance with the notification requirements of the Act if it notifies affected individuals in

accordance with its policies. If notification to more than 10,000 residents of Georgia at once is necessary, then the Covered Entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a.

The Act provides no statutory remedies or independent civil causes of action against Covered Entities who have experienced a data breach; however, violations could potentially be pursued under other legal theories such as negligence per se.

Additionally, the Federal Trade Commission (FTC) is increasingly investigating and taking enforcement action under Section 5(a) of the FTC Act, involving "unfair and deceptive trade practices," against companies that have experienced data breaches for alleged failures to take reasonable steps to secure consumers' Personal Information. Violations involving personal health care information may be investigated and prosecuted by the U.S. Department of Justice.

Given the increasing threat of identity theft, Georgia companies should focus on limiting their potential exposure. By taking steps such as updating security systems, minimizing storage of Personal Information, using unique identifying numbers, redacting and encrypting all stored Personal Information and compartmentalizing the storage of Personal Information on different network segments, businesses can help ensure they don't become the subject of the next data breach headlines.

Amy T. Andrews is an attorney with Baker, Donelson, Bearman, Caldwell & Berkowitz, PC (Atlanta). She may be reached at (404) 443-6704 or by email at aandrews@bakerdonelson.com.